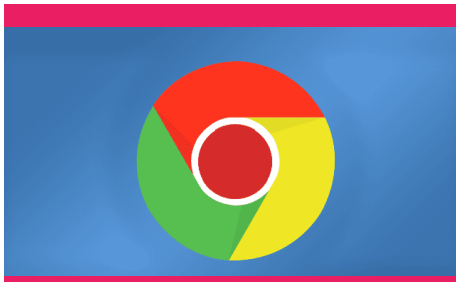
شماره شانزدهم - اردیبهشت ۱۳۹۷

خبرنامه "آپا" دانشگاه خوارزمی

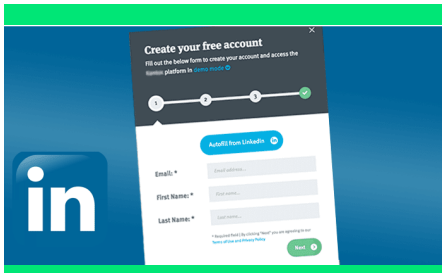
KHARAZMI CERT
COORDINATION CENTER
مرکز تخصصی آپا خوارزمی

در این شماره خواهید خواند:



بیش از ۲۰ میلیون کاربر، مسدود کننده مخرب آگهی را از فروشگاه کروم دریافت کرده‌اند!

اگر شما یکی از افزونه‌های مسدود کننده آگهی که در زیر به آن‌ها اشاره شده است را روی مرورگر کروم نصب کرده‌اید، ممکن است هک شده باشید. - صفحه ۲



نقص امنیتی در پلاگین تکمیل خودکار LinkedIn

نه تنها فیس‌بوک، بلکه در قابلیت محبوب تکمیل خودکار LinkedIn هم اخیرا یک آسیب‌پذیری کشف شده که باعث می‌شود اطلاعات حساس کاربران بدون اطلاعشان برای سایت‌های واسطه فاش شود. - صفحه ۳

آسیب پذیری بحرانی هسته سیستم مدیریت محتوای دروپال

اخیرا یک آسیب پذیری اجرای کد از راه دور در چند نسخه از سیستم مدیریت محتوای دروپال کشف گردیده است که به طور بالقوه به مهاجمان اجازه اجرای کدهای مخرب را داده و منجر به آسیب دیدگی سایت دروپال شما می‌گردد.- صفحه ۴

توصیه جهت جلوگیری فوری استفاده از رمز نگاری PGP

حفظ حریم خصوصی یک ابزار رمزگذاری است که برای امضای ایمیل، اسناد، دایرکتوری ها و حتی هارد دیسک کامل استفاده می شود. به گفته واستاد محقق امنیتی سباستین شینزل از FH Münster، رمزگذاری ایمیل PGP و S/MIMEحاوی نقصی است که اجازه می دهد تا فرم ساده بازگردانی شود. - صفحه ۵

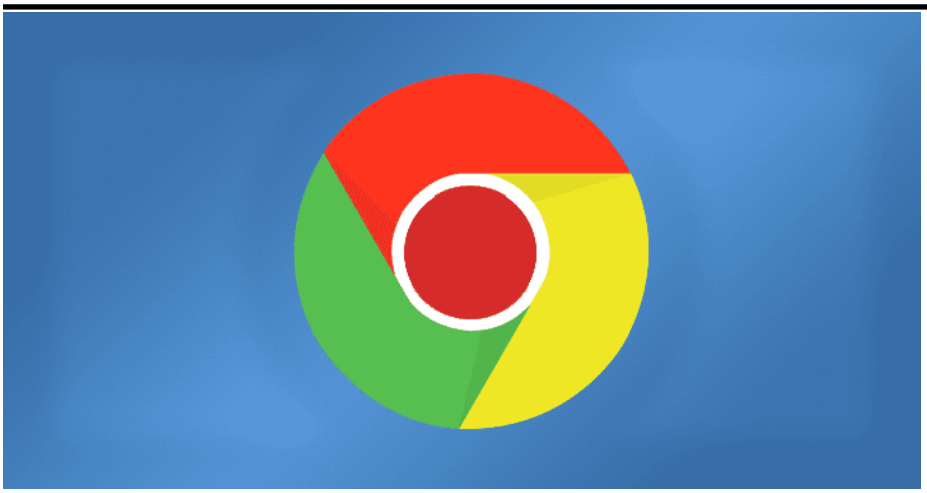
به روز رسانی سه شنبه گذشته مایکروسافت و رفع نقص موتور VBScript

بخشی از به روز رسانی مایکروسافت روز سه شنبه ، یک نقص حیاتی در ویندوزرا که به طور فعال مورد بهره برداری قرار می گرفت patch کرد. این آسیب پذیری در موتور VBScript اجازه می دهد تا سوءاستفاده از zero-day برای آلوده سازی ماشین ها به کار گرفته شود.بدین ترتیب با باز کردن اسکریپت های خاص ساخته شده می تواند صدمات جدی برای حافظه ایجاد کرده و منجر به اجرای کد دلخواه گردد. - صفحه ۶

فایرفاکس حفاظت CSRF را باپشتیبانی از کوکی‌های Same-Site بهبود می‌بخشد.

Adobeصبح روز سه شنبه چهار آسیب پذیری مهم را در محصولات Flash Player و InDesign به عنوان بخشی از بولتن امنیتی ماه آوریل April Security Bulletin که به طور منظم برنامه ریزی شده است، برطرف کرد. - صفحه ۷

بیش از ۲۰ میلیون کاربر، مسدود کننده مخرب آگهی را از فروشگاه کروم دریافت کرده‌اند!



اگر شما یکی از افزونه‌های مسدود کننده آگهی که در زیر به آن‌ها اشاره شده است را روی مرورگر کروم نصب کرده‌اید، ممکن است هک شده باشید.

یک محقق امنیتی پنج افزونه مسدود کننده مخرب آگهی را در فروشگاه کروم شناسایی کرده که دست کم توسط ۲۰ میلیون کاربر نصب شده‌اند.

متأسفانه افزونه‌های مخرب مرورگرها اغلب دسترسی به همه فعالیت‌های آنلاین شما دارند و می‌توانند هر اطلاعاتی که قربانیان در هر وبسایتی وارد می‌کنند را بدزدند. این اطلاعات ممکن است شامل کلمه عبور، تاریخچه مرور وب و جزئیات کارت اعتباری باشد.

Andrey Meshkov، یکی از بنیان‌گذاران Adguard کشف کرده است که این پنج افزونه مخرب تقلیدی از نسخه‌های برخی نرم‌افزارهای رسمی و مشهور مسدود کننده آگهی هستند.

سازندگان این افزونه‌ها همچنین از واژگان کلیدی محبوب در نام و توضیحات استفاده کرده‌اند تا جایگاه خود را در نتایج جستجو بالاتر ببرند، این موضوع می‌تواند کاربران بیشتری را برای دانلود این افزونه جذب کند.

پس از آن که Meshkov یافته‌های خود را به گوگل گزارش داد، این قول فناوری فوراً همه افزونه‌هایی که در زیر به عنوان مسدود کننده مخرب آگهی نام برده شده‌اند را از فروشگاه کروم حذف کرد:

- AdRemover for Google Chrome™ (10 million+ users)
- uBlock Plus (8 million+ users)
- [Fake] Adblock Pro (2 million+ users)
- HD for YouTube™ (400,000+ users)
- Webutation (30,000+ users)

Meshkov افزونه AdRemover را برای کروم دانلود کرد و پس از تجزیه و تحلیل آن کشف کرد کد مخرب داخل نسخه اصلاح شده jQuery، یک کتابخانه جاوااسکریپت معروف، مخفی شده است و اطلاعاتی درباره برخی سایت‌هایی که کاربر بازدید می‌کند برای سرور راه دور ارسال می‌کند.

سپس افزونه مخرب فرمان‌هایی از سرور راه دور دریافت می‌کند که در background page افزونه اجرا می‌شود و می‌تواند رفتار مرورگر شما را تغییر دهد.

برای جلوگیری از کشف شدن، این فرمان‌ها در یک فایل ظاهراً بی‌ضرر تصویری مخفی می‌شوند.

Meshkov گفت: "این فرامین اسکریپت‌هایی هستند که در وضعیت مدیریت اجرا می‌شوند و می‌توانند رفتار مرورگر شما را به هر ترتیبی تغییر دهند، اساساً این یک botnet است که از مرورگرهای آلوده شده به وسیله افزونه جعلی Adblock تشکیل شده است. مرورگر هر فرمانی را که سرور راه دور بخواهد اجرا می‌کند."

این محقق همچنین سایر افزونه‌های موجود در فروشگاه کروم را هم بررسی کرده و چهار افزونه دیگر با تاکتیک مشابه یافته است.

از آن‌جا که افزونه مرورگر مجوز دسترسی به همه صفحات وبی که شما بازدید می‌کنید را می‌گیرد، عملاً هر کاری می‌تواند بکند.

بنابراین پیشنهاد می‌کنیم حداقل افزونه‌های ممکن را روی مرورگر خود نصب کنید و این افزونه‌ها از شرکت‌های مورد اعتماد شما باشند.

گردآورنده: حسین علیمرادی

نقص امنیتی در پلاگین تکمیل خودکار LinkedIn

نه تنها فیس‌بوک، بلکه در قابلیت محبوب تکمیل خودکار LinkedIn هم اخیرا یک آسیب‌پذیری کشف شده که باعث می‌شود اطلاعات حساس کاربران بدون اطلاعشان برای سایت‌های واسطه فاش شود.

این پلاگین به سایت‌های دیگر اجازه می‌داد کاربران پروفایل خود را با استفاده از اطلاعات پروفایل LinkedIn مانند نام کامل، شماره تلفن، آدرس ایمیل، کد پستی، عنوان شغلی و شرکت را با یک کلیک کامل کنند.

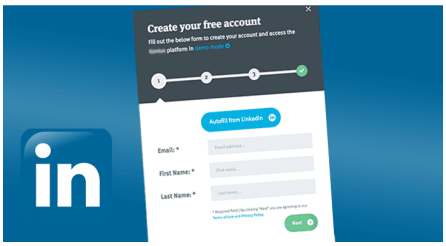
به طور کلی دکمه تکمیل خودکار در سایت‌های لیست سفید کار می‌کند اما محقق ۱۸ ساله امنیتی، Jack Cable از Lightening Security اعلام کرده است که موضوع فقط این نیست.

Cable کشف کرده است که این ویژگی یک آسیب‌پذیری امنیتی ساده اما مهم دارد که به طور بالقوه هر وب‌سایت (scraper) را قادر می‌سازد مخفیانه اطلاعات پروفایل کاربر را بدون اطلاع خودش جمع‌آوری کند.

یک وبسایت مطمئن ممکن است دکمه تکمیل خودکار را در قسمت‌های مختلف سایت قرار دهد، اما بنا به گفته Cable یک مهاجم می‌تواند مخفیانه از این ویژگی استفاده کند و با تغییر ویژگی‌های آن دکمه را در کل صفحه گسترش داده و آن را مخفی کند.

از آن‌جا که دکمه تکمیل خودکار مخفی است، کاربران با کلیک روی هر نقطه از سایت، این ویژگی را فراخوانی می‌کنند و در نهایت اطلاعات عمومی و شخصی آن‌ها به وب‌سایت مخرف ارسال می‌شود.

مهاجمان چگونه از نقص LinkedIn بهره‌برداری می‌کنند:



- کاربر از سایت مخربی بازدید می‌کند که دکمه تکمیل خودکار LinkedIn را در یک iframe باز می‌کند.

- iframe طوری طراحی شده که کل صفحه را در بر می‌گیرد و برای کاربر قابل رؤیت نیست.

- کاربر در هر نقطه‌ای از صفحه کلیک می‌کند و LinkedIn این عمل را آغاز فرآیند کلید تکمیل خودکار معنی می‌کند و داده‌های کاربر را از طریق postMessage به سایت مخرب ارسال می‌کند.

Cable این آسیب‌پذیری را در ۹ آپریل کشف کرد و بلافاصله به LinkedIn اعلام کرد. این شرکت روز بعد بدون اعلام همگانی اقدام به انتشار اصلاحیه موقت کرد.

اصلاحیه فقط استفاده از این ویژگی را به سایت‌های لیست سفید محدود کرد. این سایت‌ها، همان سایت‌هایی هستند که به LinkedIn بابت میزبانی تبلیغاتشان پول پرداخت می‌کنند. Cable معتقد است این پچ ناقص بوده و سایت‌های لیست سفید می‌توانند با سوء استفاده از این ویژگی داده‌های کاربران را جمع‌آوری کنند.

علاوه بر این هر کدام از سایت‌های این لیست ممکن است اطلاعات کاربران را در اختیار سایت‌های ثالث مخربی قرار دهند.

برای اثبات این موضوع، Cable یک صفحه‌ای ساخته‌است که نشان می‌دهد چطور یک سایت می‌تواند نام و نام خانوادگی، نشانی ایمیل، کارفرما و محل را بدست آورد.

از آن‌جا که LinkedIn اصلاحیه کاملی برای رفع این آسیب‌پذیری در تاریخ ۱۹ آپریل عرضه کرد، ممکن است صفحه گفته شده کار نکند.

این شرکت در بیانیه‌ای اعلام کرد: "ما به محض اطلاع جلوی استفاده غیرمجاز از این ویژگی را گرفتیم و در حال انتشار اصلاحیه دیگری هستیم که سایر موارد بالقوه سوءاستفاده را نیز در زمان کوتاه برطرف کند. البته هیچ نشانه‌ای از سوءاستفاده دیده نشده است و ما به طور مداوم در تلاشیم تا مطمئن باشیم داده‌های اعضای ما محافظت شده است. از گزارش مسئولانه این محققین تشکر می‌کنیم و تیم امنیت ما ارتباط با ایشان را ادامه خواهد داد."

اگر چه آسیب‌پذیری همیشه پیچیده یا بحرانی نیست، اما با توجه به رسوایی اخیر Cambridge Analytica که در آن داده‌های بیش از ۸۷ میلیون کاربر فیس‌بوک افشا شده بود، این ضعف‌های امنیت می‌تواند علاوه‌بر مشتریان برای خود شرکت هم تهدیدی جدی باشد.

گردآورنده: حسین علیمرادی

آسیب پذیری بحرانی هسته سیستم مدیریت محتوای دروپال

پروژه: Drupal core

تاریخ: ۲۵ آوریل ۲۰۱۸ – ۵ اردیبهشت ۹۷

اهمیت: بحرانی

نوع آسیب پذیری: (RCE) اجرای کد از راه دور

CVE :CVE-2018-7602

اخیرا یک آسیب پذیری اجرای کد از راه دور (RCE) در چند نسخه از سیستم مدیریت محتوای دروپال کشف گردیده است که به طور بالقوه به مهاجمان اجازه اجرای کدهای مخرب را داده و منجر به آسیب دیدگی سایت دروپال شما می‌گردد. این آسیب پذیری در نسخه‌های 7.x و 8.x وجود دارد.

پیشگیری:

دروپال خود را به جدید ترین نسخه ۷ یا ۸ ارتقاء دهید.

- اگر از نسخه 7.x استفاده میکنید به نسخه 7.59 ارتقاء دهید.
- اگر از نسخه 8.5.x استفاده میکنید به نسخه 8.5.3 ارتقاء دهید.
- اگر از نسخه 8.4.x استفاده میکنید به نسخه 8.4.8 ارتقاء دهید. (در نظر داشته باشید این نسخه از دروپال مدت زیادی است که پشتیبانی نمی‌شود با این حال به منظور تسریع در رفع این آسیب پذیری یک نسخه بروزرسانی منتشر گردیده است. در اسرع وقت نسبت به ارتقاء سیستم مدیریت محتوای خود به آخرین نسخه امن اقدام نمایید)

اگر امکان بروزرسانی فوری سایت خود را ندارید، یا از توزیع‌های دیگر دروپال استفاده می‌کنید می‌توانید از patch زیر به منظور رفع آسیب پذیری استفاده کرده و سپس در آینده سیستم خود را به طور کامل بروزرسانی کنید.

- Patch for Drupal 8.x (8.5.x and below)
- Patch for Drupal 7.x

گردآورنده: حسین علیمرادی

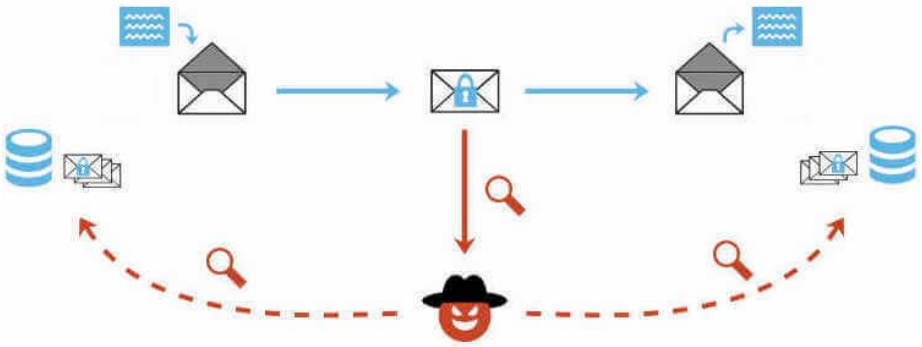
توصیه جهت جلوگیری فوری استفاده از رمز نگاری PGP

حفظ حریم خصوصی (PGP)یک ابزار رمزگذاری است که برای امضای ایمیل، اسناد، دایرکتوری ها و حتی هارد دیسک کامل استفاده می شود. به گفته واستاد محقق امنیتی سباستین شینزل از FH Münster، رمزگذاری ایمیل PGP و S/MIME حاوی نقصی است که اجازه می دهد تا فرم ساده بازگردانی شود.

این مسئله نگرانی بسیار مهم برای کسانی است که از این رمزگذاری برای محافظت از اطلاعات حساس استفاده می کنند. پیش از این ایمیل رمزگذاری شده ممکن است جهت رمزگشایی در دسترس قراربگیرد. حتی فرد برای انجام این کار به مجوز های لازم (دسترسی ها ی لازم) نیاز نخواهد داشت.

اگرچه تحقیقات رسمی مورد نظر تا روز سه شنبه ساعت ۷ صبح UTC منتشر نخواهد شد، اما بنیاد Electronic Frontier پیش از دسترسی به انتشار گزارش کامل پیش از موعد به منظور هشدار دادن این خطر به جامعه اقدام کزده است. Schninzel و سایر اعضای تیمش نیز عملا به عنوان بخشی از مسئولیت آگاهی رسانی پیش از زمان مشخص شده به کاربران هشدار داده بودند.

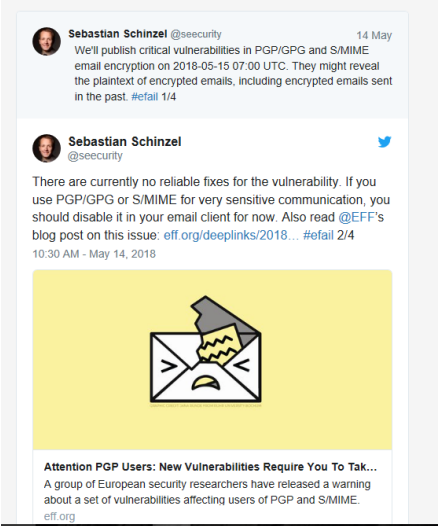
هر دو تیم محققان Schninzel و تمیش و EFF که در این پروژه فعالیت میکنند توصیه می کنند که تمام کاربران PGP بلافاصله ابزار مورد استفاده خود را غیرفعال یا حذف



کنند تا مسائل مطرح شده مورد بررسی دقیق قرار گیرد. هنوز هم اعتقاد بر این است که جایگزین هایی مانند سیگنال جزء روش های امن ارتباطی هستند.

در حال حاضر هیچ رفع نقص قابل اعتمادی برای این آسیب پذیری وجود ندارد. در صورت استفاده از PGP/GPG یا S/MIME برای ارتباط بسیار حساس، در حال حاضر باید آن را در سرویس ایمیل خود غیر فعال کنید. همچنین پست وبلاگ EFF در این مورد را بخوانید:

https://t.co/zJh2YHhE5q#efail2/4



در حال حاضر هیچ اصلاحاتی برای رفع نقایص مورد بحث پیدا نشده است. در حال حاضر می‌دانیم که می بایست استفاده از روش‌های PGP و S/MIME متوقف گردد، تا اطلاعات بیشتری برای ادامه حیات این روش رمز گذاری به دست آید.

گردآورنده: سمیه نیاخلیلی

به روز رسانی سه شنبه گذشته مایکروسافت و رفع نقص موتور VBScript

بخشی از به روز رسانی مایکروسافت روز سه شنبه ، یک نقص حیاتی در ویندوزرا که به طور فعال مورد بهره برداری قرار می گرفت patch کرد. این آسیب پذیری در موتور VBScript اجازه می دهد تا سوءاستفاده از zero- day برای آلوده سازی ماشین ها به کار گرفته شود.بدین ترتیب با باز کردن اسکریپت های خاص ساخته شده می تواند صدمات جدی برای حافظه ایجاد کرده و منجر به اجرای کد دلخواه گردد. در یک حمله مبتنی بر وب، صفحات مخصوص طراحی شده می توانند از آسیب پذیری مشابه هنگام استفاده از اینترنت اکسپلورر استفاده کنند. جاسازی کردن کنترل های AcitveX که "در زمان اجرا امن برای راه اندازی مجدد" می باشد در داخل یک سند مایکروسافت آفیس قرار گرفته و کد ناامن بعد از استفاده از موتور رندر IE آن را به اجرا می گذارد. یکی از بخش های جالب تر این حمله این است که مهم نیست مرورگر پیش فرض کاربر چه چیزی باشد. هنگام استفاده از VBScript، می توان یک صفحه وب را با استفاده از اینترنت اکسپلورر مجبور کرد حتی اگر Chrome، FireFox، Safari، Opera یا مرورگر دیگری به طور پیش فرض به عنوان مرورگر اصلی تنظیم شده باشد. این آسیب پذیری خاص در ویندوز ۷، ویندوز سرور ۲۰۰۸ وسیستم عامل های جدیدتر تاثیر گزار خواهد بود.

آزمایشگاه کسپرسکی یک تجزیه و تحلیل دقیق از عملکرد توابع بهره برداری ارائه کرده است. به طور خلاصه، یک بیانیه از سوی محققان امنیتی بیان می دارد که: "ما انتظار داریم این آسیب پذیری در آینده نزدیک به یکی از بیشترین سوء استفاده های مورد استفاده برسد، زمان زیادی نخواهد گذشت که سازندگان کیت از آن سوءاستفاده نکنند. در هر دو طرف (توسط مرورگر) و مبارزات فیشینگ (از طریق اسناد) مورد استفاده قرار خواهد گرفت."

مایکروسافت علاوه بر کشف نقص VBScriptو پچ کردن آن ازتشدید آسیب پذیری جلوگیری کرده است.شکست کامپوننت Win32k اجازه می دهد تا هر کد دلخواه در حالت کرنل اجرا شود. این مجوز و دسترسی برای یک حساب کاربری استاندارد موجب دستیابی به دسترسی کامل به سیستم میگردد، هر چند باید اشاره کرد که کاربر می بایست برای اعمال سوء استفاده به سیستم وارد شود. در این مورد، هر دو سوءاستفاده پچ شده اند ، اما به این معنا نیست که کاربران نهایی و مدیران، سیستم های خود را به صورت اتوماتیک ودر فواصل برنامه ریزی شده به روز رسانی کنند. توصیه می شود که به روز رسانی ها به صورت دستی انجام گیرد تا مطمئن شوند آخرین patch ها نیز نصب شده اند. در مجموع، ۶۷ بروز رسانی ۲۱ آسیب پذیری با درجه اهمیت بحرانی را برطرف کرده اند.

گردآورنده: سمیه نیاخلیلی

فایرفاکس حفاظت CSRF را با پشتیبانی از کوکی‌های Same-Site بهبود می‌بخشد.

Adobe صبح روز سه شنبه چهار آسیب پذیری مهم را در محصولات Flash Player و InDesign به عنوان بخشی از بولتن امنیتی ماه آوریل April Security Bulletin که به طور منظم برنامه ریزی شده است، برطرف کرد.

مهندسین موزیلا در حال برنامه‌ریزی برای افزودی یک ویژگی امنیتی جدید به فایرفاکس با افزودن پشتیبانی از کوکی‌های Same-Site در فایرفاکس ۶۰ هستند. انتشار این نسخه برای ۹ می سال جاری برنامه‌ریزی شده است. ویژگی کوکی Same-Site باعث می‌شود دانلود کوکی‌هایی که متعلق به سایر دامنه‌هایی هستند که با URL فعلی نوار آدرس مرورگر فایرفاکس مطابقت ندارند مسدود شود.

توسعه دهندگان فایرفاکس می‌گویند ویژگی Same-Site برای حفاظت از کاربران در برابر حملات درخواست جعلی بین سایتی CSRF طراحی شده است. حملات CSRF زمانی اتفاق می‌افتد که مهاجمان کاربران را فریب می‌دهند تا اقداماتی انجام دهند اما عملیات دیگری در پس‌زمینه انجام می‌دهند. برای مثال یک کاربر ممکن است روی یک لینک مخرب کلیک کند، اما مهاجم از این کلیک برای تغییر در تنظیمات حساب در یک سایت دیگر با استفاده از کوکی‌های محلی استفاده می‌کند.

این موضوع معمولاً به این دلیل اتفاق می‌افتد که مرورگرها به صورت خودکار کوکی‌های ارسال شده با هر درخواستی از سوی مرورگر را برای یک دامنه خاص پیوست می‌کنند. مهاجمان با سوء استفاده از مکانیزم "افزودن خودکار کوکی" درخواست‌هایی برای سایت‌های دیگر می‌سازند و به طور مؤثر کوکی‌های ذخیره شده در کامپیوتر کاربر را به سرقت می‌برند، حتی زمانی که کاربر در سایتی دیگر باشد، تا بدون آن که کاربران بدانند از آن‌ها برای عملیات مخرب استفاده کنند.

به دلیل ساختار فعلی تکنولوژی وب، برنامه‌های تحت وب و وبسایت‌ها نمی‌توانند به صورت مطمئن اقدامات یک کاربر واقعی را از کارهایی که توسط اسکریپت‌های خودکار انجام می‌شوند تشخیص دهند. با افزودن پشتیبانی از کوکی‌های Same-Site در فایرفاکس، یک گزینه جدید برای کاربران اضافه می‌شود که می‌توانند با تنظیم آن برای برنامه‌ها و پورتال‌ها مانع حملاتی از این دست شوند.

اما این یک گزینه امنیتی نیست که به کاربران یا موزیلا بستگی داشته باشد. ویژگی Same-Siteباید توسط مالکان سایت‌ها در سرصفحه پاسخ HTTP تنظیم شود، مشابه روشی که برای تنظیم کوکی‌ها استفاده می‌شود.

براساس مشخصات IETF، دو تنظیم برای اپراتور سایت‌ها در دسترس خواهد بود، Strict و Lax

زمانی که یک مالک سایت از «Strict» در سایتش استفاده کند، فایرفاکس کوکی‌هایی با درخواست HTTP با دامنه‌هایی جز URL فعلی که در نوار آدرس باشد را نمی‌پذیرد.

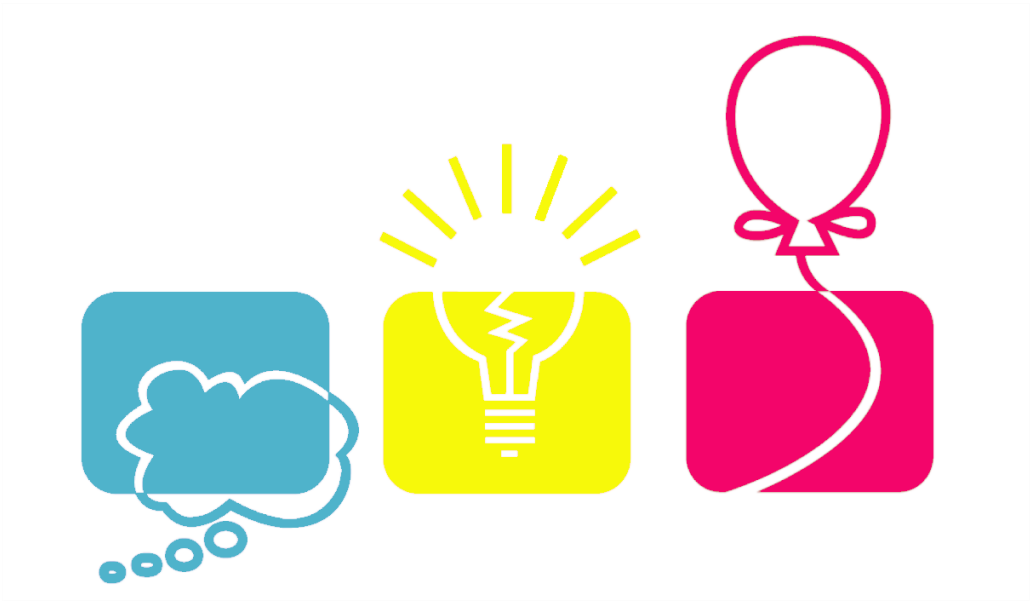
برای گزینه «Lax» اگر کاربر با یک روش امن به سایت رسیده باشد، فایرفاکس کوکی‌هایی با سایر دامنه‌ها را بارگزاری می‌کند. روش امن مانند کلیک یا دنبال کردن یک لینک است. برای مثال اگر کاربر در Facebook باشد و روی لینک domain.com باشد و domain.com با سیاست کوکی سایت-مشابه Lax باشد، کوکی‌های domain.com و Facebook هر دو بارگزاری می‌شوند اما باز هم دریافت کوکی‌هایی از آدرس‌هایی به جز این دو آدرس مقدور نخواهد بود.

برای اطلاعات بیشتر درباره چگونگی استفاده از این ویژگی توسط صاحبان سایت را می‌توانید در مشخصات IETF RFC ۶۲۶۵ مشاهده کنید.

کروم این ویژگی را از دسامبر سال ۲۰۱۷ و نسخه ۶۳ خود اضافه کرده بود. دیگر مرورگرهایی که از قابلیت پشتیبانی می‌کنند اپرا (از نسخه ۵۱ به بعد)، کروم اندروید (از نسخه ۶۴ به بعد و Samsung Internet از نسخه ۶,۲ به بعد) هستند.

گردآورنده: حسین علیمرادی

KHARAZMI CERT COORDINATOR CENTER



مرکز آپا دانشگاه خوارزمی

رییس مرکز:

دکتر امید مهدی عبادتی

اعضای هیات علمی:

دکتر احسان ملکیان

دکتر امید مهدی عبادتی

کارشناسان مرکز:

محمدحسین خدامی

سمیه نیا خلیلی

محمد مرتضوی

امین زمانی

حسین علیمرادی

شیوا بهادری

محسن نادری

محسن یزدی‌نژاد

نشانی:

کرج - دانشگاه خوارزمی - کتابخانه‌ی مرکزی - طبقه‌ی همکف - مرکز آپا

تلفن:

۰۲۶۳۴۵۷۵۰۱۲

۰۲۶۳۴۵۷۵۰۱۸

۰۲۶۳۴۵۷۹۶۰۰ (داخلی ۲۶۲۲)

پست الکترونیک:

cert@khu.ac.ir

وب سایت:

http://cert.khu.ac.ir/

کانال مرکز آپا خوارزمی:

@khu_cert

دانلود رایگان:

دانلود رایگان مجموعه کامل خبرنامه‌ها از طریق اسکن کد زیر در دسترس است.